THERE IS CLAIMED:

1. A method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network, comprising:

establishing an association between a mobile terminal (MT) and an access point (AP);

establishing an authentication channel between the AP and an Internet service provider (ISP); and

communicating AAA messages, to effect said AAA transactions, between the MT and the AP, and between the AP and the ISP;

wherein said processing of said AAA transactions is performed using only IP layer functions.

2. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein said communicating of said AAA messages comprises:

until an affirmative authentication determination, filtering all traffic from the MT at the AP so that the traffic is not passed beyond the AP;

sending an Internet service provider (ISP) identifier and a user identifier (UID) from the MT to the AP;

sending the UID from the AP to the ISP indicated by the ISP identifier;

at the ISP, randomly generating a string S_1 and encrypting S_1 with a password of the user to provide encrypted version SS^1;

sending S_1 and SS^1 from the ISP to the AP;

storing SS^1 at the AP;

sending S_1 from the AP to the MT;

at the MT, encrypting S_1 with the password of the user to provide encrypted version SS_1, and randomly generating a second string S_2;

sending SS_1 and S_2 from the MT to the AP;

making the authentication determination at the AP, wherein:

when $SS^1 = SS_1$, the authentication determination is affirmative,

only when the authentication determination is affirmative, sending the UID, SS_1, and S_2 from the AP to the ISP;

at the ISP, only when $SS^1 = SS_1$:

accepting access by the MT;

encrypting S_2 with the password of the user to provide encrypted version SS^2, and

sending SS^2 from the ISP to the AP;

sending SS^2 from the AP to the MT;

at the MT:

decrypting SS^2 to provide a decrypted version S^2 of the second string from the ISP; and

sending subsequent traffic to the AP only when $S_2 = S^2$;

wherein, when the authorization determination is affirmative, the subsequent traffic from the MT is passed beyond the AP without the filtering.

3. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 2, wherein the step of sending SS^2 from the AP to the MT also includes sending to the MT a session key and a broadcast key, and wherein the session key is used for encryption of the subsequent messages from the MT.

4. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein communications between the MT and the AP are performed over an air interface complying with the IEEE 802.11 standard.

5. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as

set forth in claim 1, wherein communications between the MT and the AP are performed over an air interface complying with the Bluetooth standard.

6. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein communications between the MT and the AP are performed over an air interface complying with the HiperLAN2 standard.

7. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein communications between the MT and the AP are performed over an air interface complying with the homeRF standard.

8. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein communications between the MT and the AP are performed over an air interface complying with a cellular 3G standard.

9. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as

set forth in claim 1, wherein communications between the MT and the AP are performed without modification to any layer 2 standard protocols.

10. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein IPSEC is used for per-packet encryption of messages from the MT.

11. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 1, wherein an IPSEC authentication header is used for per-packet authentication of messages from the MT.

12. A method for an access point (AP) to support authentication, authorization and accounting (AAA) transactions in a wireless network, comprising:

accepting an association with a mobile terminal (MT);

establishing an authentication channel with an Internet service provider (ISP); and

receiving AAA messages sent from the MT, and sending corresponding AAA messages to the ISP, to effect said AAA transactions;

wherein processing of said AAA transactions is performed using only IP layer functions.

13. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein said receiving and said sending of said AAA messages comprises:

until an affirmative authentication determination, filtering all traffic from the MT so that the traffic is not passed beyond the AP;

receiving an Internet service provider (ISP) identifier and a user identifier (UID) from the MT;

sending the UID from the AP to the ISP indicated by the ISP identifier;

receiving a first encrypted string SS^1 and a first string S_1 from the ISP;

sending S_1 to the MT;

receiving from the MT a second encrypted string SS_1;

when $SS^1 = SS_1$:

making the affirmative authentication determination,

sending the UID and SS_1 to the ISP, and

passing subsequent traffic from the MT without the filtering.

14. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 13, further comprising:

when receiving from the MT the second encrypted string SS_1, receiving also a second string S_2; and

when sending the UID and SS_1 to the ISP, sending also S_2.

15. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 13, further comprising, when $SS^1 = SS_1$, sending to the MT a session key, wherein the session key is used for decryption of the subsequent messages from the MT.

16. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the AP performs wireless communications over an air interface complying with the IEEE 802.11 standard.

17. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the AP

performs wireless communications over an air interface complying with the Bluetooth standard.

18. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the AP performs wireless communications over an air interface complying with the HiperLAN2 standard.

19. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the AP performs wireless communications over an air interface complying with the homeRF standard.

20. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the AP performs wireless communications over an air interface complying with a cellular 3G standard.

21. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein the

communication of the AAA messages is performed without modification to layer 2 protocols of the standards.

22. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein IPSEC is used for per-packet decryption of the subsequent messages from the MT.

23. The method for an AP to support authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 12, wherein an IPSEC authentication header is used for per-packet authentication of the subsequent messages from the MT.

24. A method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network, comprising:

establishing an association between a mobile terminal (MT) and an access point (AP);

assigning the MT a dynamic IP address;

until an affirmative authentication determination, filtering all traffic from the dynamic IP address at the AP so that the traffic is not passed beyond the AP;

sending a user initiated login message, from the MT to the AP, including an Internet service provider (ISP) identifier and a user identifier (UID);

sending an access request message, from the AP to the ISP indicated by the ISP identifier, including the UID;

at the ISP, randomly generating a string S_1 and encrypting S_1 with a password of the user to provide encrypted version SS^1;

sending an access challenge message, from the ISP to the AP, including S_1 and SS^1;

storing SS^1 at the AP;

sending a forwarded access challenge message, from the AP to the MT, including S_1;

at the MT, encrypting S_1 with the password of the user to provide encrypted version SS_1, and randomly generating a second string S_2;

sending an access challenge MT response message, from the MT to the AP, including SS_1 and S_2;

making the authentication determination at the AP, wherein:

when $SS^1 = SS_1$, the authentication determination is affirmative,

when the authentication determination is affirmative, sending a follow up access request message, from the AP to the ISP, including the UID, SS_1, and S_2;

when the authentication determination is not affirmative:

ignoring the access challenge MT response message, and

awaiting another access challenge MT response message from the MT;

making an access acceptance determination at the ISP, wherein:

when $SS^1 = SS_1$, the access is accepted by the ISP;

when the access is accepted by the ISP:

encrypting S_2 with the password of the user to provide encrypted version SS^2, and

sending an access accept message, from the ISP to the AP, including SS^2;

when the access is not accepted by the ISP, sending an access reject message from the ISP to the AP;

in response to the access accept message, sending a forwarded access accept message, from the AP to the MT, including SS^2;

at the MT, making a trust determination with respect to the AP and ISP, comprising:

decrypting SS^2 to provide a decrypted version S^2 of the second string from the ISP; and

when $S_2 = S^2$, the trust determination is affirmative;

wherein, when the authorization determination is affirmative and the trust determination is affirmative, subsequent traffic from the dynamic IP address is passed beyond the AP without the filtering.

25. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein processing of said AAA transactions is performed using only IP layer functions.

26. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein the forwarded access accept message includes a session key and a broadcast key, and the session key is used for encryption of the subsequent messages from the MT.

27. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications between the

MT and the AP are performed over an air interface complying with the IEEE 802.11 standard.

28. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications between the MT and the AP are performed over an air interface complying with the Bluetooth standard.

29. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications between the MT and the AP are performed over an air interface complying with the HiperLAN2 standard.

30. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications between the MT and the AP are performed over an air interface complying with the homeRF standard.

31. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications between the

MT and the AP are performed over an air interface complying with a cellular 3G standard.

32. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein communications during the sending steps are performed without modification to any layer 2 standard protocols.

33. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein IPSEC is used for per-packet encryption of messages from the MT.

34. The method for effecting authentication, authorization and accounting (AAA) transactions in a wireless network as set forth in claim 24, wherein an IPSEC authentication header is used for per-packet authentication of messages from the MT.

35. A method for effecting accounting in a wireless network, comprising:

sending traffic from the MT over the Internet via the AP; and

performing decentralized accounting of the traffic by producing mutual accounting proofs at the MT and the AP.

36. The method for effecting accounting as set forth in claim 35, wherein the method does not include sending packets of the MT through a central virtual operator server.

37. The method for effecting accounting as set forth in claim 35, wherein the producing of mutual accounting proofs comprises:

monitoring the traffic at the MT and the AP to produce respective traffic profiles; and

making a comparison between the traffic profiles.

38. The method for effecting accounting as set forth in claim 37, further comprising sending a verified profile to an ISP based on at least one of the traffic profiles when the comparison indicates a match between the traffic profiles.

39. The method for effecting accounting as set forth in claim 38, wherein the comparison indicates the match

between the traffic profiles based on the traffic profiles differing by an amount within a predetermined threshold.

40. The method for effecting accounting as set forth in claim 37, further comprising blocking the traffic from the MT when the comparison indicates no match between the respective traffic profiles.

41. The method for effecting accounting as set forth in claim 37, wherein, when the comparison indicates no match between the respective traffic profiles, the AP permits the MT to adopt the respective traffic profile of the AP.

42. The method for effecting accounting as set forth in claim 41, wherein, when the MT does not adopt the respective traffic profile of the AP, the traffic from the MT is blocked.

43. An access point (AP) for a wireless network, comprising a processor and a memory under control of the processor, the memory having instructions enabling the processor to perform the steps of:

accepting an association with a mobile terminal (MT);

establishing an authentication channel with an Internet service provider (ISP); and

receiving AAA messages sent from the MT, and sending corresponding AAA messages to the ISP, to effect said AAA transactions;

wherein processing of said AAA transactions is performed using only IP layer functions.

44. The access point as set forth in claim 43, wherein said receiving and said sending of said AAA messages comprises:

until an affirmative authentication determination, filtering all traffic from the MT so that the traffic is not passed beyond the AP;

receiving an Internet service provider (ISP) identifier and a user identifier (UID) from the MT;

sending the UID from the AP to the ISP indicated by the ISP identifier;

receiving a first encrypted string SS^1 and a first string S_1 from the ISP;

sending S_1 to the MT;

receiving from the MT a second encrypted string SS_1;

when $SS^1 = SS_1$:

making the affirmative authentication determination,

sending the UID and SS_1 to the ISP, and

passing subsequent traffic from the MT without the filtering.

45. The access point as set forth in claim 44, further comprising:

when receiving from the MT the second encrypted string SS_1, receiving also a second string S_2; and

when sending the UID and SS_1 to the ISP, sending also S_2.

46. The access point as set forth in claim 44, further comprising, when $SS^1 = SS_1$, sending to the MT a session key, wherein the session key is used for decryption of the subsequent messages from the MT.

47. The access point as set forth in claim 43, wherein the AP performs wireless communications over an air interface complying with the IEEE 802.11 standard.

48. The access point as set forth in claim 43, wherein the AP performs wireless communications over an air interface complying with the Bluetooth standard.

49. The access point as set forth in claim 43, wherein the AP performs wireless communications over an air interface complying with the HiperLAN2 standard.

50. The access point as set forth in claim 43, wherein the AP performs wireless communications over an air interface complying with the homeRF standard.

51. The access point as set forth in claim 43, wherein the AP performs wireless communications over an air interface complying with a cellular 3G standard.

52. The access point as set forth in claim 43, wherein the communication of the AAA messages is performed without modification to layer 2 protocols of the standards.

53. The access point as set forth in claim 43, wherein IPSEC is used for per-packet decryption of the subsequent messages from the MT.

54. The access point as set forth in claim 43, wherein an IPSEC authentication header is used for per-packet authentication of the subsequent messages from the MT.